Сибирский математический журнал
Сентябрь—октябрь, 2002. Том 43, № 5

УДК 512.5

КОНЕЧНЫЕ ГРУППЫ ОГРАНИЧЕННОГО РАНГА С ПОЧТИ РЕГУЛЯРНЫМ АВТОМОРФИЗМОМ ПРОСТОГО ПОРЯДКА

Е. И. Хухро

Аннотация: Доказывается, что если конечная группа ранга r допускает автоморфизм φ простого порядка, имеющий ровно m неподвижных точек, то она обладает φ-инвариантной подгруппой (r, m)-ограниченного индекса, которая нильпотентна r-ограниченной ступени (теорема 1). Тем самым для случая автоморфизма простого порядка усиливаются ранее полученные результаты Шалева, Хухро и Хайкина-Запирайна. Доказательство основано, в частности, на результате о регулярных автоморфизмах колец Ли (теорема 3). По модулю известных результатов общий случай сводится к случаю конечных p-групп. Для сведения к кольцам Ли используются также мощные p-группы, для которых доказывается полезный факт, позволяющий «склеивать» ступени нильпотентности факторов определенных нормальных рядов (теорема 2).

Ключевые слова: конечная группа, ранг, автоморфизм, почти регулярный, мощная p-группа, кольцо Ли, нильпотентный

1. Введение

Пусть φ — автоморфизм конечной группы G. Классические теоремы Томпсона [1] и Хигмэна — Крекнина — Кострикина [2–4] утверждают, что если порядок φ — простое число p и φ действует без нетривиальных неподвижных точек, т. е. *регулярно*, то группа G нильпотентна и ее ступень нильпотентности ограничена в терминах p (или, короче, *p-ограничена*). В более общей ситуации результаты о *почти регулярных* автоморфизмах ограничивают строение группы G в зависимости от числа $m = |C_G(\varphi)|$ неподвижных точек автоморфизма φ. В работах [5–10] доказано (по модулю классификации конечных простых групп), что если $|C_G(\varphi)| = m$ для автоморфизма φ простого порядка p, то группа G содержит подгруппу (p, m)-ограниченного индекса, которая нильпотентна p-ограниченной и m-ограниченной ступени.

Заключения вышеупомянутых результатов зависят от порядка автоморфизма. В другом направлении, если задаться ограничением на ранг группы G, удается получить результаты о строении группы G с почти регулярным автоморфизмом, *не зависящие* от порядка автоморфизма. Напомним, что *рангом* конечной группы G называется наименьшее число r такое, что любая подгруппа группы G порождается r элементами. А. Шалев [11] доказал (используя классификацию конечных простых групп), что если конечная группа ранга r

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 99–01–00576) и гранта Минобразования РФ в области фундаментального естествознания (код проекта Е00–1.0–77).

допускает автоморфизм, имеющий ровно m неподвижных точек, то она обладает разрешимой подгруппой (r,m)-ограниченного индекса, причем если порядок автоморфизма взаимно прост с порядком группы, то эту подгруппу можно выбрать разрешимой (r,m)-ограниченной ступени. В [12] мы усилили вторую часть теоремы Шалева, показав, что в случае взаимно простых порядков подгруппу (r,m)-ограниченного индекса можно выбрать разрешимой r-ограниченной ступени. Наконец, в работе Хайкина-Запирайна [13] рассмотрен «модулярный» случай p-автоморфизма конечной p-группы ранга r и также доказано существование подгруппы (r,m)-ограниченного индекса, которая разрешима r-ограниченной ступени.

Целью настоящей работы является усиление этих результатов для случая автоморфизма простого порядка. Именно, доказывается, что если в описанной ситуации порядок автоморфизма — простое число, то имеется подгруппа (r,m)-ограниченного индекса, которая нильпотентна r-ограниченной ступени. (Подчеркнем, что здесь ограничения индекса и ступени нильпотентности не зависят от порядка автоморфизма в отличие от заключений результатов, процитированных в первом абзаце, зависящих от порядка автоморфизма.)

Теорема 1. *Если конечная группа G ранга r допускает автоморфизм φ простого порядка, имеющий ровно m неподвижных точек, то она обладает φ-инвариантной подгруппой (r,m)-ограниченного индекса, которая нильпотентна r-ограниченной ступени. При $m=1$, т. е. когда автоморфизм φ регулярен, группа G нильпотентна r-ограниченной ступени.*

Мы не стремились выписать явные оценки функций, участвующих в формулировке теоремы, хотя это вполне может быть сделано. Так же, как в [11], доказательство теоремы основано, в частности, на результате о регулярных автоморфизмах колец Ли (теорема 3). Если в [11] обобщалась теорема Крекнина [4] о регулярном автоморфизме кольца Ли, то здесь мы обобщаем теорему Крекнина и Кострикина [3]. По модулю известных результатов доказательство теоремы 1 сводится к случаю конечных p-групп. Для сведения к кольцам Ли используются также мощные p-группы [14]. Для них мы доказываем полезный факт, позволяющий «склеивать» ступени нильпотентности факторов некоторых нормальных рядов (теорема 2).

Используемые обозначения по большей части стандартны. Отметим без доказательства следующие две хорошо известные леммы, которые будут рутинно использоваться без особых ссылок. Здесь и далее индуцированный автоморфизм фактор-группы мы обозначаем той же буквой.

Лемма 1. *Пусть G — конечная группа, а φ — ее автоморфизм порядка, взаимно простого с порядком G. Если N — нормальная φ-инвариантная подгруппа, то $C_{G/N}(\varphi)=C_G(\varphi)N/N$.* $\square$

Лемма 2. *Пусть G — конечная группа, а φ — ее автоморфизм. Если N — нормальная φ-инвариантная подгруппа, то $|C_{G/N}(\varphi)|\leq|C_G(\varphi)|$.* $\square$

2. Мощные p-группы

Напомним определения и свойства мощных p-групп. Через G^n обозначается подгруппа группы G, порожденная всеми n-ми степенями элементов из G.

Определения. Нормальная подгруппа N конечной p-группы G называется *мощно вложенной*, если $N^p\geq[N,G]$ при нечетном p (если $N^4\geq[N,G]$ при

$p = 2$). Конечная p-группа G называется *мощной*, если она мощно вложена в себя, т. е. если $G^p \geq [G, G]$ при $p \neq 2$ (если $G^4 \geq [G, G]$ при $p = 2$).

Лемма 3 [14, теорема 1.1]. *Если M, N — мощно вложенные подгруппы конечной p-группы G, то M^p, MN и $[M, N]$ также мощно вложены.* □

В частности, все члены ряда коммутантов, нижнего центрального ряда, их степени и другие коммутаторно-степенные подгруппы мощной p-группы являются мощно вложенными подгруппами. Эти факты будут использоваться без особых ссылок. Следующий результат указывает на роль мощных p-групп в теории групп конечного ранга.

Лемма 4 [14, теоремы 1.14, 4.14]. *Любая конечная p-группа G ранга r содержит характеристическую мощную подгруппу Q такую, что $|G : Q| \leq p^{r(\log_2 r+2)}$.* □

Приведем еще несколько свойств мощных p-групп.

Лемма 5 [14, § 1]. *Пусть G — мощная p-группа.*

Для каждого i подгруппа G^{p^i}, порожденная всеми p^i-ми степенями, на самом деле состоит из p^i-х степеней; при этом $(G^{p^i})^{p^j} = G^{p^{i+j}}$ для всех i, j.

Подгруппы G^{p^i} образуют центральный ряд, причем $[G^{p^i}, G^{p^j}] \leq G^{p^{i+j}}$ для всех i, j.

Секции $G^{p^i}/G^{p^{i+1}}$ являются элементарными абелевыми группами для всех i. Взятие p-х степеней индуцирует гомоморфизм секции $G^{p^i}/G^{p^{i+1}}$ на $G^{p^{i+1}}/G^{p^{i+2}}$ и потому $|G^{p^i}/G^{p^{i+1}}| \geq |G^{p^{i+1}}/G^{p^{i+2}}|$ для всех i. □

Следующая лемма Шалева (одно из включений было уже в [14]) позволяет переставлять операции взятия степеней и взаимных коммутантов мощно вложенных подгрупп.

Лемма 6. [15, лемма 3.1]. *Если M, N — мощно вложенные подгруппы конечной p-группы G, то $[M^p, N] = [M, N]^p$.* □

Теперь докажем теорему, которая позволяет для мощных p-групп «склеивать» ступени нильпотентности факторов некоторых нормальных рядов (что, конечно, невозможно в общем случае).

Теорема 2. *Предположим, что мощная p-группа P обладает рядом длины t вида*

$$P > P^{p^{k_1}} > P^{p^{k_2}} > \dots > P^{p^{k_t}} = 1,$$

в котором все факторы $S = P^{p^{k_i}}/P^{p^{k_{i+1}}}$ удовлетворяют соотношению $\gamma_v(S^{p^u})=1$ для некоторых одних и тех же натуральных чисел u, v. Тогда $\gamma_{g(t,v)}(P^{p^{f(t,u)}})=1$, где $f(t, u)$ — некоторое (t, u)-ограниченное число, а $g(t, v) = v^t + v^{t-1} + \dots + v$.

Доказательство. Индукция по t. По предположению индукции

$$\gamma_g(P^{p^f}) \subseteq P^{p^k}, \tag{1}$$

где $g = g(t-1, v)$, $f = f(t-1, u)$ и $k = k_{t-1}$. Кроме того, по условию

$$\gamma_v((P^{p^k})^{p^u}) = 1.$$

Применяя лемму 6 к левой части последнего равенства, получаем

$$\gamma_v(P)^{p^{vk+vu}} = 1. \tag{2}$$

Будем искать $f(t,u)$ в виде $f+w$. Тогда нам нужно получить равенство

$$\gamma_{gv+v}(P^{p^{f+w}})=1.$$

По лемме 6 преобразуем последовательно левую часть, используя (1):

$$\begin{aligned}\gamma_{gv+v}(P^{p^{f+w}}) &= (\gamma_{gv+v}(P^{p^f}))^{p^{(gv+v)w}} \le ([P^{p^k},\underbrace{P^{p^f},\dots,P^{p^f}}_{g(v-1)+v}])^{p^{(gv+v)w}}\\ &= ([P,\underbrace{P^{p^f},\dots,P^{p^f}}_{g(v-1)+v}]^{p^k})^{p^{(gv+v)w}} \le (\gamma_{g(v-1)+v}(P^{p^f})^{p^k})^{p^{(gv+v)w}}\\ &\le ([P^{p^k},\underbrace{P^{p^f},\dots,P^{p^f}}_{g(v-2)+v}]^{p^k})^{p^{(gv+v)w}}\\ &= ([P,\underbrace{P^{p^f},\dots,P^{p^f}}_{g(v-2)+v}]^{p^{2k}})^{p^{(gv+v)w}} \le \dots \le (\gamma_v(P^{p^f})^{p^{vk}})^{p^{(gv+v)w}}\\ &= \gamma_v(P)^{p^{vf+vk+(gv+v)w}}.\end{aligned}$$

Для того чтобы правая часть стала равна 1, согласно (2) достаточно, чтобы

$$vf+vk+(gv+v)w \ge vk+vu,$$

т. е. $w \ge (u-f)/(g+1)$. Ясно, что такое w можно выбрать меньше u, так что $f(t,u)=f+w$ останется (t,u)-ограниченным числом. $\square$

Теперь дадим определение специального класса мощных p-групп, которые обладают еще более линейными свойствами.

Определение. Пусть p^t — период мощной p-группы G, т. е. t — наименьшее число такое, что $G^{p^t}=1$. Если для всех $i\le t-1$ справедливы равенства $|G/G^p|=|G^{p^i}/G^{p^{i+1}}|$, то группа G называется *однообразно мощной.*

Лемма 7. *Пусть G — однообразно мощная p-группа периода p^t. Тогда для каждого $i=0,1,\dots,t-2$ отображение $x\to x^p$ индуцирует изоморфизм секции $G^{p^i}/G^{p^{i+1}}$ на $G^{p^{i+1}}/G^{p^{i+2}}$.*

3. Кольцо Ли с автоморфизмом простого порядка

Напомним некоторые стандартные обозначения и терминологию. Для подмножеств A, B кольца Ли через $[A,B]$ обозначается аддитивная подгруппа, порожденная всеми коммутаторами (произведениями) $[a,b]$, где $a\in A$, $b\in B$. Коммутатор $[\dots[[a_1,a_2],a_3],\dots,a_n]$ называется *простым* и обозначается через $[a_1,a_2,\dots,a_n]$. Аналогичное обозначение используется для подмножеств:

$$[\dots[[A_1,A_2],A_3],\dots,A_n]=[A_1,A_2,\dots,A_n].$$

Члены ряда коммутантов кольца Ли L определяются рекурсивно как

$$L^{(1)}=[L,L],\quad L^{(n+1)}=[L^{(n)},L^{(n)}].$$

Члены нижнего центрального ряда обозначаются через

$$\gamma_n(L)=[\underbrace{L,\dots,L}_{n}].$$

Аддитивная группа $\gamma_n(L)$ порождается всеми простыми коммутаторами веса n от элементов кольца L.

Любое кольцо Ли L можно считать кольцом над целыми числами $\mathbb{Z}$. Если ω — первообразный корень n-й степени из 1, то тензорное произведение $L \otimes \mathbb{Z}[\omega]$ естественным образом становится кольцом Ли над $\mathbb{Z}[\omega]$; любой автоморфизм φ кольца L естественным образом становится автоморфизмом кольца $L \otimes \mathbb{Z}[\omega]$. Автоморфизм φ порядка n кольца Ли L называется *полупростым*, если после вышеописанного расширения основного кольца аддитивная группа L разлагается в прямую сумму аналогов подпространств собственных векторов преобразования φ:

$$L = \bigoplus_{i=0}^{n-1} L_i,$$

где $L_i = \{l \in L \mid l^{\varphi} = \omega^i l\}$ — аддитивная подгруппа, называемая *φ-компонентой, отвечающей собственному значению* ω^i. Вопреки обыкновению в этом контексте мы используем термин «собственное значение», даже если $L_i = 0$.

Теорема 3. *Предположим, что кольцо Ли L допускает полупростой автоморфизм φ простого порядка, имеющий ровно d различных собственных значений с ненулевыми φ-компонентами, причем все эти собственные значения не равны* 1 *(т. е. автоморфизм φ регулярен). Тогда кольцо Ли L нильпотентно ступени, не превосходящей* $\frac{d^{2^{d-1}-1}-1}{d-1}$.

Доказательство теоремы 2 состоит в применении теоремы Шалева [11], где получена оценка $2^{d-1}-1$ для ступени разрешимости кольца Ли L, и следующей теоремы, являющейся обобщением теоремы Крекнина и Кострикина [3].

Теорема 4. *Предположим, что кольцо Ли L допускает полупростой автоморфизм φ простого порядка, имеющий ровно d различных собственных значений с ненулевыми φ-компонентами, причем все эти собственные значения не равны* 1. *Тогда*

(а) $[\gamma_k([L,L]), \underbrace{L,\dots,L}_{d}] \subseteq \gamma_{k+1}([L,L])$ *для любого натурального k;*

(б) $\gamma_{dk+2}(L) \subseteq \gamma_{k+1}([L,L])$ *для любого натурального k;*

(в) *для любого натурального n имеем $\gamma_{f(d,n)+1}(L) \subseteq L^{(n)}$, где $f(d,n) = \frac{d^n-1}{d-1}$.*

Доказательство. Нам потребуется следующая элементарная теоретико-числовая лемма из [3].

Лемма 8 [3]. *Пусть $i_1,\dots,i_d$ — ненулевые не обязательно различные элементы простого поля $\mathbb{F}_q$ из q элементов, где q — простое число. Образуем множество*

$$M = \Big\{\sum_{j\in S} i_j \mid S \subseteq \{1,\dots,d\}\Big\},$$

включая $\sum\limits_{j\in\varnothing} i_j = 0$. Тогда либо $M = \mathbb{F}_q$, либо $|M| \geq d+1$. $\square$

(а) Пусть $|\varphi| = q$, где q — простое число. Можно, очевидно, считать, что основное кольцо содержит первообразный корень q-й степени из единицы ω. Для каждого $i = 0,1,\dots,q-1$ пусть $L_i = \{l \in L \mid l^{\varphi} = \omega^i l\}$ — φ-компонента, отвечающая собственному значению ω^i (не исключая возможности $L_i = 0$). Тогда по условию $L = \bigoplus_{i=0}^{q-1} L_i$. Легко проверить, что при этом

$$[L_i, L_j] \subseteq L_{i+j(\operatorname{mod} q)} \tag{3}$$

для всех i, j. Аналогичное разложение имеет место и для любого φ-инвариантного подкольца.

По условию $L_i \neq 0$ только для d различных ненулевых значений i. Пусть $i_1, \ldots, i_d$ — все такие значения. Нам достаточно показать, что

$$[a_{i_0}, l_{j_1}, \ldots, l_{j_d}] \equiv 0 \ (\operatorname{mod} \gamma_{k+1}([L, L])) \tag{4}$$

для любых $a_{i_0} \in L_{i_0} \cap \gamma_k([L, L])$, $l_{j_k} \in L_{j_k}$, где $j_k \in \{i_1, \ldots, i_d\}$. Мы используем здесь индексы только для указания той φ-компоненты, которой принадлежит элемент вида l_{j_k}, т. е. одинаковые символы здесь могут обозначать разные элементы из одной и той же φ-компоненты. Элементы $l_{j_1}, \ldots, l_{j_d}$ можно произвольным образом переставлять в (4), не нарушая сравнения по модулю $\gamma_{k+1}([L, L])$. По лемме 8 таким образом в качестве суммы (по модулю q) индексов нескольких первых элементов включая a_{i_0} можно получить не менее $d + 1$ различных значений. В силу (3) соответствующие коммутаторы — начальные отрезки коммутатора (4) при таких перестановках — будут лежать в φ-компонентах, отвечающих этим $d + 1$ собственным значениям автоморфизма φ. По условию хотя бы одна из этих φ-компонент равна 0, что и доказывает сравнение (4).

(б) Индукция по k. При $k = 1$ это утверждение (а) для $k = 1$. При $k > 1$ по предположению индукции имеем

$$\gamma_{dk+2}(L) = [\gamma_{d(k-1)+2}(L), \underbrace{L, \ldots, L}_{d}] \subseteq [\gamma_k([L, L]), \underbrace{L, \ldots, L}_{d}] \subseteq \gamma_{k+1}([L, L]),$$

где во втором включении снова использовано утверждение (а).

(в) Индукция по n. При $n = 1$ имеем $\gamma_{f(d,1)+1}(L) = \gamma_2(L) = L^{(1)}$. При $n > 1$ будет

$$\gamma_{f(d,n)+1}(L) = \gamma_{df(d,n-1)+2}(L) \subseteq \gamma_{f(d,n-1)+1}([L, L])$$

согласно (б). Теперь мы применяем к правой части предположение индукции для φ-инвариантного подкольца $[L, L]$:

$$\gamma_{f(d,n-1)+1}([L, L]) \subseteq [L, L]^{(n-1)} = L^{(n)},$$

что и завершает доказательство теоремы 4. □

Завершим доказательство теоремы 3. По теореме Шалева [11] кольцо Ли L разрешимо ступени $2^{d-1} - 1$. Остается применить часть (в) теоремы 4 при $n = 2^{d-1} - 1$. □

Хотя в дальнейшем нам потребуется сама теорема 3, отметим следствие для колец Ли с аддитивной группой ограниченного ранга.

Следствие. *Предположим, что аддитивная группа кольца Ли L имеет ранг r. Если кольцо Ли L допускает регулярный полупростой автоморфизм φ простого порядка, то кольцо Ли L нильпотентно ступени, не превосходящей* $\frac{r^{2^{r-1}-1}-1}{r-1}$. □

4. Случай конечной p-группы

Здесь мы докажем теорему 1 для конечных p-групп. Пусть G — конечная p-группа ранга r, φ — ее автоморфизм простого порядка q, и пусть $|C_G(\varphi)| = m$.

Сначала рассмотрим случай $p \neq q$. Мы должны выделить случай $m = 1$, поскольку тогда мы не можем прибегнуть к взятию подгруппы (r, m)-ограниченного индекса, так как индекс любой собственной подгруппы делится на p. На самом деле мы докажем, что тогда сама группа G нильпотентна r-ограниченной ступени. Этот результат будет также использован в общей ситуации.

Теорема 5. *Если конечная группа G ранга r допускает регулярный автоморфизм φ простого порядка, то группа G нильпотентна r-ограниченной ступени, не превосходящей* $\frac{r^{2^{r-1}-1}-1}{r-1}$.

Доказательство. По теореме Томпсона [1] группа G нильпотентна, так что достаточно рассмотреть случай, когда G — конечная p-группа. Ясно, что $|\varphi| \neq p$. По лемме 1 автоморфизм φ индуцирует регулярный автоморфизм присоединенного кольца Ли $L(G)$, который обозначается той же буквой. Этот автоморфизм полупрост в силу того, что порядок φ взаимно прост с p. Мы, однако, не можем применить следствие из теоремы 3, так как ранг аддитивной группы $L(G)$ нельзя предполагать r-ограниченным. Вместо этого мы применим теорему 3, предварительно показав, что φ имеет только r-ограниченное число различных собственных значений на $L(G)$. Все эти значения не равны 1, так как автоморфизм φ регулярен. (Здесь мы снова говорим о собственном значении, только подразумевая, что соответствующая φ-компонента ненулевая.)

По теореме Шалева [11] группа G разрешима r-ограниченной ступени. Каждый фактор ряда коммутантов группы G — абелева p-группа ранга $\leq r$. Поэтому на каждой из них φ также действует полупросто и имеет не более r различных собственных значений после расширения основного кольца первообразным корнем q-й степени из единицы ω. Значит, и в совокупности на всех факторах ряда коммутантов φ имеет некоторое r-ограниченное число собственных значений.

Для любого фактора нижнего центрального ряда $A = \gamma_i(G)/\gamma_{i+1}(G)$ пересечения $\gamma_i(G)$ с членами ряда коммутантов индуцируют естественные гомоморфизмы $\mathbb{Z}\langle\varphi\rangle$-модулей — факторов ряда коммутантов — на факторы индуцированного ряда, связывающего $\gamma_i(G)$ и $\gamma_{i+1}(G)$. Эти гомоморфизмы индуцируют гомоморфизмы и соответствующих $\mathbb{Z}[\omega]\langle\varphi\rangle$-модулей. Поэтому при действии на A автоморфизм φ может иметь только те собственные значения, что встречаются при действии φ на факторах ряда коммутантов. Следовательно, при действии на факторах нижнего центрального ряда в совокупности φ имеет только r-ограниченное число собственных значений. Это означает, что φ имеет r-ограниченное число собственных значений при действии на кольце $L(G)$, чья аддитивная группа равна прямой сумме факторов нижнего центрального ряда. Тогда по теореме 3 кольцо Ли $L(G)$ нильпотентно r-ограниченной ступени. Значит, и группа G нильпотентна той же ступени. $\square$

Продолжим доказательство теоремы 1 для p-групп при $p \neq q = |\varphi|$. Рассмотрим теперь случай, когда $m = |C_G(\varphi)| > 1$. Так как $m = p^n$ для некоторого $n \geq 1$, число p ограничено в терминах m и мы можем переходить к соответствующим подгруппам. По лемме 4 группа G содержит мощную характеристическую подгруппу (r, p)-ограниченного, а значит, и (r, m)-ограниченного индекса. Поэтому можно с самого начала считать p-группу G мощной.

Рассмотрим ряд неравенств

$$|G/G^p| \geq |G^p/G^{p^2}| \geq \cdots \geq |G^{p^i}/G^{p^{i+1}}| \geq \ldots,$$

которые выполняются для порядков элементарных абелевых секций $G^{p^i}/G^{p^{i+1}}$ по лемме 5. Так как их ранги не превосходят r, в этом ряду может быть не более r строгих неравенств. Участки рассматриваемого ряда с равенствами соответствуют секциям вида $G^{p^a}/G^{p^{a+b}}$, которые являются однообразно мощными p-группами. Таким образом, группа G обладает рядом

$$G > G^{p^{a_1}} > \cdots > G^{p^{a_l}} = 1, \tag{5}$$

где все факторы — однообразно мощные p-группы, а их число не превосходит r.

Пусть $K = G^{p^a}/G^{p^{a+b}}$ — любой из однообразно мощных факторов ряда (5); его период равен p^b. Ясно, что K — φ-инвариантная секция группы G. По лемме 7 отображение $x \to x^p$ индуцирует изоморфизмы $\mathbb{Z}\langle\varphi\rangle$-модулей $G^{p^{a+i}}/G^{p^{a+i+1}}$ для всех $i = 0, 1, \ldots, b-1$. Поэтому, а также по лемме 1 централизатор φ в K либо тривиален, либо имеет период p^b. В последнем случае, очевидно, $p^b \leq m = |C_G(\varphi)|$, так что тогда период секции K не превосходит m. Если же φ регулярен на K, то по теореме 5 ступень нильпотентности группы K ограничена в терминах r. Объединяя, получаем, что в любом случае

$$\gamma_{c(r)}(K^m) = 1, \tag{6}$$

где $c(r)$ — некоторое r-ограниченное число.

Доказательство теоремы 1 в случае p-групп при $p \neq q$ завершается применением теоремы 2. Напомним, что $m = p^n$. По теореме 2 из (6) вытекает, что для соответствующих функций $\gamma_{g(r,c(r))}(G^{p^{f(r,n)}}) = 1$, т. е. φ-инвариантная подгруппа $G^{p^{f(r,n)}}$ нильпотентна ступени $g(r, c(r)) - 1$. Число $g(r, c(r))$ ограничено в терминах r. Индекс подгруппы $G^{p^{f(r,n)}}$ ограничен в терминах r и m, так как период фактор-группы $G/G^{p^{f(r,m)}}$ ограничен в терминах r и m (напомним, что $p \leq m$), а ее ранг не превосходит r.

Рассмотрим теперь «модулярный» случай, когда $p = q$, т. е. φ — автоморфизм порядка p конечной p-группы G. Так как $C_G(\varphi) \neq 1$, здесь всегда $p \leq m$, причем $m = p^n$ для некоторого натурального n. По тем же причинам, что и выше, p-группу G можно считать мощной и имеющей ряд

$$G > G^{p^{a_1}} > \cdots > G^{p^{a_l}} = 1, \tag{7}$$

где все факторы — однообразно мощные p-группы, а их число не превосходит r. Пусть снова $K = G^{p^a}/G^{p^{a+b}}$ — любой из однообразно мощных факторов ряда (7); его период равен p^b.

Лемма 9. *Либо период K не превосходит p^{2n+3}, либо ранг K не меньше $p-1$.*

Доказательство. Положим $u = [(b+1)/2]$, где p^b — период K. По лемме 5 подгруппа $U = K^{p^u}$ абелева. Множество $V = \{u^{-1}u^{\varphi} \mid u \in U\}$, как легко проверить, является подгруппой. Так как φ действует тривиально на U/V, по лемме 2 имеем $|U/V| \leq m = p^n$. Значит, $U^{p^n} \leq V$. Для любого $v \in V$ найдется $u \in U$ такой, что $v = u^{-1}u^{\varphi}$; тогда

$$vv^{\varphi}v^{\varphi^2}\ldots v^{\varphi^{p-1}} = u^{-1}u^{\varphi}(u^{-1}u^{\varphi})^{\varphi}\ldots(u^{-1}u^{\varphi})^{\varphi^{p-1}} = 1. \tag{8}$$

Предположим, что $b > 2n+3$. Тогда период подгруппы U не меньше p^{n+2}, а период U^{p^n} не меньше p^2. Выберем любой элемент $a \in U^{p^n}$ порядка p^2. Подгруппа $A = \langle a, a^{\varphi}, \dots, a^{\varphi^{p-1}} \rangle$, т. е. $\mathbb{Z}\langle\varphi\rangle$-подмодуль из K, порожденный элементом a, является гомоморфным образом свободного однопорожденного $\mathbb{Z}\langle\varphi\rangle$-модуля аддитивного периода p^2 со свободным порождающим x, т. е. свободной абелевой группы ранга p периода p^2

$$F = \langle x \rangle \oplus \langle x^{\varphi} \rangle \oplus \dots \oplus \langle x^{\varphi^{p-1}} \rangle.$$

В силу тождества (8) ядро этого гомоморфизма содержит подгруппу $D = \langle x x^{\varphi} \dots x^{\varphi^{p-1}} \rangle$. Легко подсчитать, что $|C_{F/D}(\varphi)| = p$. По лемме 2 тогда во всех фактор-группах по φ-инвариантным подгруппам из F/D число неподвижных точек автоморфизма φ равно p. Отсюда вытекает, что все φ-инвариантные подгруппы группы F/D образуют линейно упорядоченное множество по включению. Так как подгруппа $F^p D/D$ является φ-инвариантной, а период A равен p^2, получаем, что ядро нашего гомоморфизма содержится в $F^p D/D$. Поэтому ранг группы A равен $p-1$. $\square$

Если период каждого фактора ряда (7) не превосходит p^{2n+3}, то порядок группы G ограничен в терминах r и m (напомним, что $p^n = m$). В противном случае по лемме 9 хотя бы один из факторов ряда (7) имеет ранг не меньше $p-1$. Следовательно, в этом случае $p-1 \leq r$, т. е. число p ограничено в терминах r. Тогда можно применить теорему из [8], по которой группа G содержит подгруппу (p,m)-ограниченного, а значит, и (r,m)-ограниченного индекса, которая нильпотентна p-ограниченной, а значит, и r-ограниченной ступени. (Оценка ступени нильпотентности в [8] была $h(p)+1$, где $h(p)$ — значение функции Хигмэна; в [16] эта оценка снижена до неулучшаемой $h(p)$.) $\square$

5. Завершение доказательства теоремы 1

Пусть G — конечная группа ранга r, φ — ее автоморфизм простого порядка q, и пусть $|C_G(\varphi)| = m$. По теореме Шалева [11] группу G можно считать разрешимой. Для завершения доказательства теоремы 1 достаточно показать, что подгруппа Фиттинга $F(G)$ группы G (которая φ-инвариантна) имеет (r,m)-ограниченный индекс. Тогда к каждой из φ-инвариантных силовских p-подгрупп из $F(G)$ можно применить либо теорему 5, если φ на ней регулярен, либо теорему 1, уже доказанную для случая p-группы. Произведение всех тех φ-инвариантных подгрупп (r,m)-ограниченного индекса и r-ограниченной ступени нильпотентности, которые получаются во втором случае, и всех тех силовских p-подгрупп из $F(G)$, на которых автоморфизм φ регулярен, и будет искомой подгруппой (r,m)-ограниченного индекса, которая нильпотентна r-ограниченной ступени.

Итак, докажем, что индекс $|G : F(G)|$ ограничен в терминах r и m. Если порядок $|\varphi| = q$ делит порядок G, то φ имеет нетривиальные неподвижные точки (на φ-инвариантной силовской q-подгруппе группы G). Тогда q делит m и можно применить теорему Хартли — Майкснера [6], по которой индекс $F(G)$ ограничен в терминах q и m, а значит, и (r,m)-ограничен (даже m-ограничен).

Пусть теперь $|\varphi| = q$ не делит $|G|$. Тогда стандартные рассуждения в духе теорем типа Холла — Хигмэна (см., например, [6, лемма] или [12, § 2]) дают, что

1) либо φ действует тривиально на $G/F(G)$,

2) либо G обладает φ-инвариантной элементарной абелевой секцией T, являющейся свободным $\mathbb{F}_t\langle\varphi\rangle$-модулем для некоторого простого t,

3) либо (в так называемом исключительном случае) G обладает φ-инвариантной экстраспециальной секцией S, являющейся s-группой для некоторого простого s, в которой φ действует тривиально на $Z(S)$ и точно на $S/Z(S)$.

В случае 1 имеем $|G/F(G)| \leq m$ по лемме 1.

В случае 2 порядок φ, очевидно, ограничен в терминах размерности пространства T, а значит, и в терминах r.

В случае 3 число $s = |Z(S)|$ не превосходит m по лемме 1. Тогда порядок элементарной абелевой s-группы $S/Z(S)$ ранга $\leq r$ ограничен в терминах r и m. Следовательно, (r,m)-ограничен и порядок автоморфизма φ, точно действующего на $S/Z(S)$.

В случаях 2 и 3 порядок автоморфизма φ ограничен в терминах r и m. Значит, снова можно применить теорему Хартли — Майкснера [6], по которой индекс $|G : F(G)|$ ограничен в терминах r и m. Теорема 1 доказана. $\square$

ЛИТЕРАТУРА

1. *Thompson J. G.* Finite groups with fixed-point-free automorphisms of prime order // Proc. Nat. Acad. Sci. USA. 1959. V. 45. P. 570–581.

2. *Higman G.* Groups and rings which have automorphisms without non-trivial fixed elements // J. London Math. Soc. 1957. V. 32. P. 321–334.

3. *Крекнин В. А., Кострикин А. И.* Алгебры Ли с регулярными автоморфизмами // Докл. АН СССР. 1963. Т. 149. С. 249–251.

4. *Крекнин В. А.* Разрешимость алгебр Ли с регулярными автоморфизмами конечного периода // Докл. АН СССР. 1963. Т. 150. С. 467–469.

5. *Fong P.* On orders of finite groups and centralizers of p-elements // Osaka J. Math. 1976. V. 13. P. 483–489.

6. *Hartley B., Meixner T.* Finite soluble groups containing an element of prime order whose centralizer is small // Arch. Math. (Basel). 1981. V. 36. P. 211–213.

7. *Alperin J.* Automorphisms of solvable groups // Proc. Amer. Math. Soc. 1962. V. 13. P. 175–180.

8. *Хухро Е. И.* Конечные p-группы, допускающие автоморфизм порядка p с малым числом неподвижных точек // Мат. заметки. 1985. Т. 38, № 5. С. 652–657.

9. *Хухро Е. И.* Кольца Ли и группы, допускающие почти регулярный автоморфизм простого порядка // Мат. сб. 1990. Т. 181, № 9. С. 1207–1219.

10. *Medvedev Yu.* p-Divided Lie rings and p-groups // J. London Math. Soc. (2). 1999. V. 59. P. 787–798.

11. *Shalev A.* Automorphisms of finite groups of bounded rank // Israel J. Math. 1993. V. 82. P. 395–404.

12. *Хухро Е. И.* Почти регулярные автоморфизмы конечных групп ограниченного ранга // Сиб. мат. журн. 1996. Т. 37, № 6. С. 1407–1412.

13. *Jaikin-Zapirain A.* Finite groups of bounded rank with an almost regular automorphism // Israel J. Math. (to appear).

14. *Lubotzky A., Mann A.* Powerful p-groups. I: finite groups // J. Algebra. 1987. V. 105. P. 484–505.

15. *Shalev A.* On almost fixed point free automorphisms // J. Algebra. 1993. V. 157. P. 271–282.

16. *Макаренко Н. Ю.* Почти регулярные автоморфизмы простого порядка // Сиб. мат. журн. 1992. Т. 33, № 5. С. 206–208.

Статья поступила 2 августа 2001 г.

Хухро Евгений Иванович
Институт математики им. С. Л. Соболева СО РАН, Новосибирск 630090
khukhro@math.nsc.ru